UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/662,811	09/16/2003	Hendrik Gerlach	1454.1501	1111

21171 7590 04/14/2008

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
04/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/662,811	GERLACH ET AL.	
	Examiner	Art Unit	
	LONGBIT CHAI	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 29.

Response to Argument

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, Applicant asserts Ott does not teach "an external display to display the current security status of the appliance directly on the outside of the appliance" (Remarks: Page 7 / 5th Para). Examiner respectfully disagrees because (a) Ott teaches the network security system / server can display the current network status in virtually real-time to an operator of the system such as a display monitor of the security server (Ott: Para [0043]) and (b) Examiner note a network security status event is also qualified as a server security status event, e.g., as shown in (Ott: Para [0026] / Table 1: Line 4 & Line 7 - 8) such as (i) login attempts and/or failures and (ii) any event, process, or status of successful or unsuccessful Information connection to the network by computers within the network and (c) the monitor display is indeed directly on an outside of the server (Ott: Figure 1 / Element 110).

4. As per claim 1, Applicant asserts Ott does not teach "an internal display to display the current security status of the appliance within the inside of the appliance" (Remarks: Page 9 / 3rd Para). Examiner respectfully disagrees because (a) Ott teaches an event may be a component of a known attack signature or any detectable event associated with the protected network and the sensor agents communicate event data back to the respective security server for analysis and processing (Ott: Para [0020] Line 5 – 11 and Table 1 : Last 4 – 6 Lines) and (b) Examiner notes the event log must thus be captured, stored and identified as an event log inside the

security server where the security status identified as an internal event log of a server is qualified as an internal display of the server – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 – 4, 6 – 9, 11 – 16, 18 – 21, 23 – 27 and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Ott et al. (U.S. Patent 2004/0049698).

As per claim 1, 13 and 25, Ott teaches a system comprising:

an appliance-internal unit to detect a current security status of an appliance (Ott: Para [0043] and Para [0020] Line 1 – 15);

an external display to display the current security status of the appliance directly on the outside of the appliance (Ott: Para [0043] and Para [0026] / Table 1: Line 4 & Line 7 - 8: (a) Ott teaches the network security system / server can display the current network status in virtually real-time to an operator of the system such as a display monitor of the security server (Ott: Para [0043]) and (b) Examiner note a network security status event is also qualified as a server security status event, e.g., as shown in (Ott: Para [0026] / Table 1: Line 4 & Line 7 - 8) such as

(i) login attempts and/or failures and (ii) any event, process, or status of successful or unsuccessful Information connection to the network by computers within the network and (c) the monitor display is indeed directly on an outside of the server (Ott: Figure 1 / Element 110);

an internal display to display the current security status of the appliance within the inside of the appliance (Ott: Para [0020] Line 5 – 11 and Table 1 : Last 4 – 6 Lines: Last 4 – 6 Lines: (a) Ott teaches an event may be a component of a known attack signature or any detectable event associated with the protected network and the sensor agents communicate event data back to the respective security server for analysis and processing (Ott: Para [0020] and Table 1 : Last 4 – 6 Lines) and (b) Examiner notes the event log must thus be captured, stored and identified as an event log inside the security server where the security status identified as an internal event log of a server is qualified as an internal display of the server – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences); and

a transmission unit to transmit security status data between other appliances in a network of appliances such that the current security status data can be subjected to data processing in the network of appliances (Ott: Para [0020] / [0043]).

As per claim 2 and 14, Ott teaches the appliances are automation appliances (Ott: Para [0020]).

As per claim 3, 15 and 26, Ott teaches the external display visually displays the security status (Ott: Para [0043]: the security status is displayed in real-time to an operator).

As per claim 4, 16 and 27, Ott teaches an access unit to run automation user programs on the internal display (Ott: Para [0043] and Para [0020] Line 5 – 11: the internal event data log qualified as an internal display – This is also consistent with the specification of the instant application specification that states “the internal display” may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences))

As per claim 6 and 18, Ott teaches a joint display to display an overall security status of a plurality of appliances, respectively having their internal displays linked (Ott: Para [0028] last sentence & Para [0029] Line 10 – 15: collaborative fusion display is a joint display).

As per claim 7 and 19, Ott teaches the joint display is an external visual display (Ott: Para [0043]: the security status is displayed in real-time to an operator).

As per claim 8 and 20, Ott teaches there are a plurality of joint displays, each displaying the status of a different plurality of appliances (Ott: Para [0028] last sentence & Para [0029] Line 10 – 15 and Para [0043]), and the overall security status is passed on from the joint display to a higher-level joint display that displays an overall security status of the appliances communicating with the joint displays (Ott: Para [0042] and Para [0029] last sentence: (a) using local security zone manager and (b) collaborative agents (or fusion agents) can be configured for distribution from one security server to another security server – i.e. hierarchically linked).

As per claim 9 and 21, Ott teaches there are a plurality of joint displays, each displaying the status of a different plurality of appliances (Ott: Para [0042] and Para [0029] last sentence: (a) using local security zone manager and (b) collaborative agents (or fusion agents) can be

configured for distribution from one security server to another security server – i.e. hierarchically linked).

As per claim 11 and 23, Ott teaches a portion of the appliances have internal security mechanisms, a portion of the appliances are without internal security mechanisms, and the system integrates appliances without internal security mechanisms with appliances that have internal security mechanisms (Ott: Para [0028] Line 10 – 18 and Para [0041] last sentence & Figure 4: (a) each fusion agent is specialized in a potential network security issue – i.e. a portion of the appliances have a specific internal security mechanisms, a portion of the appliances are without those specific internal security mechanisms and (b) receiving security data directly from a keyboard instead of a communication port is considered as a method that merely dumps system events to an administrator to sort through and make sense of the data without internal intelligent security mechanism).

As per claim 12 and 24, Ott teaches the transmission unit transmits current security status via an Intranet and/or the Internet (Ott: Para [0016]).

As per claim 29, Ott teaches the internal display functions as an input for other devices within the appliance (Ott: Para [0023] Line 10 – 15).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art

to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 5, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ott et al. (U.S. Patent 2004/0049698), in view of Grainger (U.S. Patent 6,910,135).

As per claim 5, 17 and 28, Ott does not disclose expressly an internal-information base to provide access to the security status from the network of appliances via standard protocols.

Grainger teaches an internal-information base to provide access to the security status from the network of appliances via standard protocols (Grainger: Column 3 Line 18 – 23 / Line 32 – 36: SNMP / MIB (Management Information base) is used by an event correlation engine as a common information base and standard protocol for managing network events such as security status).

Accordingly, Ott in view of Grainger teaches an internal-information base to provide access to the security status from the network of appliances via standard protocols, access to the current security status being provided by the internal display (See the reasons set forth above).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grainger within the system of Ott because (a) Ott teaches detecting and presenting the network security and intrusion information relating to a series of security violations to a user by collecting the event logs through the sensor agents that communicate event data logs back to thhe respective security server for analysis and processing (Ott: Para [0020]) and (b) Grainger teaches providing an effective use of SNMP / MIB (Management Information base) by an event correlation engine as a common information base and standard protocol for managing network events such as security status (Grainger: Column 3 Line 18 – 23 / Line 32 – 36).

7. Claims 10 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ott et al. (U.S. Patent 2004/0049698), in view of Douglas (U.S. Patent 2004/0049693).

As per claim 10 and 22, Ott does not disclose expressly the security status of the internal display can be simulated such that the internal display is active even without the appliance-internal unit detecting the current security status.

Douglas teaches the security status of the internal display can be simulated such that the internal display is active even without the appliance-internal unit detecting the security status (Douglas : Para [0089]: for debugging and testing purpose – This also appears in the application specification).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Douglas within the system of Ott because (a) Ott teaches detecting and presenting the network security and intrusion information relating to a series of security violations to a user by collecting the event logs through the sensor agents that communicate event data logs back to thhe respective security server for analysis and processing (Ott: Para [0020]) and (b) Douglas teaches host-based intrusion detection system (HIDS) that monitors, simulates, tests and debugs the system logs for evidence of malicious or suspicious application activity and detects attacks targeted at the host system on which it is installed and monitors output to the system and audit logs (Douglas : Abstract and Para [0089]).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Examiner, Art Unit 2131
4/11/2008